MICROSOFT PKI IMPLEMENTATION

PKI DESIGN, IMPLEMENTATION AND OPERATION USING MICROSOFT TECHNOLOGIES

CERTIFICATION AUTHORITY DESIGN AND IMPLEMENTATION, CUSTOM PKI APPLICATION DEVELOPMENT, SMART CARD DEPLOYMENT AND ADMINISTRATION.

[CERTIFICATION AUTHORITY IMPLEMENTATION]

A certification authority (CA) is a trusted source of electronic certificates that can be used in a wide range of key security technologies based on asymmetric cryptography, such as:

- Integrated multi-factor user authentication (authentication using a certificate in a smart card)
- Web portal andweb service security through server certificates
- User authentication for websites and web services through client certificates
- Computer, service and mobile device authentication through certificates
- E-mail security - digital signatures, encryption
- Network communication encryption (IPSEC)
- Code signing, e.g. signing of company Office macros, PowerShell scripts, installation packages, Java archives, ...)
- File encryption through EFS (Encrypting File System)

For Microsoft Active Directory networks, we offer certification authority implementation based on Active Directory Certificate Services (AD CS).

FEATURES AND BENEFITS

- Close integration between MS PKI and other Microsoft technologies
- Integrated multi-factor authentication using smart cards
- Wide range of certificate utilization in security technologies
- MS Active Directory integration
- Optional registration authority applications and certificate issuance process automation
- Requires no additional software or client licenses
- Optional extension of built-in capabilities through custom applications

[ADVANTAGES OF ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)]

AD CS is a free component of Windows Server. Its installation and operation requires no additional server or client licenses.
Another fundamental benefit is the close integration with other Microsoft server and client technologies and applications, such as the certificate-based authentication integrated in Windows, the publication of user certificates into Active Directory, automated issuing and renewals of both user and computer certificates, etc.

[CERTIFICATION AUTHORITY IMPLEMENTATION DESIGN]

Certification authority implementation includes both the relevant SW and HW product deployment and the analysis and design of all related technical and administrative processes that together make up the so-called Public Key Infrastructure (PKI). The PKI implementation design includes the following:

- Analysis of the customer's environment and security needs linked to the deployment of PKI technologies
- Certification authority architecture design - root and issuing authorities, time validity design, certification authority private key security using hardware security modules (HSM), etc.
- Design of certification policies and certificate types for selected technologies that use certificates
- Design of processes for issuing client and server certificates and for CA management and operation
- Design of certificate authority, administration and backup configuration
- Configuration of the Active Directory environment and group policies for PKI and related technologies operation
- CA implementation and operation support - audit, verification, CA certificate renewal, disaster recovery

[CUSTOM DEVELOPMENT OF PKI APPLICATIONS]

For existing or implemented PKI we offer custom application and tool development and consultation concerning their development. These could be tools for easier PKI technology operation and administration - e.g. applications for issuing special types of certificates, web applications for certification authority operators (registration authorities), and web services for internal business application access to the certificate authority services, etc.

Consider ICZ CaNotifier, for example - this application monitors the certification authority's database and sends notification e-mails to users if approaching user or server certificate expiration is detected.

Another example is the custom web service mediating user certificate issuing, based on an MS certification authority, for a company ERP system.

We also offer the development of end-user applications or components for other applications performing cryptographic functions, such as encryption or data electronic signing.

[SMART CARDS]

A contact smart card is offered as secure storage for user certificates and private keys. Safe, 2-factor authentication (physical token ownership + PIN knowledge) is achieved by means of an authentication certificate in a smart card.

Smart card benefits

- Safe storage for certificates and private keys (it is impossible to copy the keys from the card)
- Safe, 2-factor user authentication for Windows and web applications
- Optional additional secret information storage (passwords and keys for different applications)

HID Crescendo C700 chip cards manufactured by HID Global are offered as standard.

A smart card can be in the format of a classic plastic card or a USB token that does not need a reader.

Smart card administration

ICardManager, providing registration and administration of the contact part, is available for the offered smart cards.

Basic parameters of the smart card contact section

- JAVA card
- EEPROM capacity 80 kB
- 2048-bit RSA key support
- SHA1/2, AES 256, and ECC algorithm support
- Crypto API, PKCS#11 cryptographic interface support
- Windows integration through SafeSign middleware (the middleware is included in the card price)

Cards are supplied in combination with an independent contactless part of an optional technology (iClass, HID, Mifare)

Program basic functions

- Card registration (serial number, PIN, PUK, etc.)
- Card initialization and PIN, PUK modification
- Card assignment to Active Directory users
- Card certificate enrolment
- Printing of handover records
- PIN unblocking
- Remote PIN unblocking by phone (using challenge-response codes)
- The software can be customized according to the customer's needs.

COMMERCIAL CONTACT

ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz